

REGULATIONS

holding, within the framework of Stage II of the II Open International Olympiad in Informatics, a competition on comprehensive solutions to cybersecurity problems

TECHNICAL TASK

1. In the Windows operating system environment (7, 8, 10, 11), there are two resident programs “merdan” and “maksat”. The following is known about these programs:

- a) programs are located in different folders of the “TEST” directory;
- b) programs are launched through one of the registry keys;
- c) programs lock the registry from time to time;
- d) programs are protected from normal deletion;
- e) each program monitors the state of the neighboring process every 100 milliseconds and restores it when deleted.

Task: You should delete these two processes (1 point), registry entries about loading these processes (1 point), unlock the registry (1 point), physical process data files located in the specified folder (1 point for each file).

Note: Deleting other files in the specified “TEST” folder, other registry keys, or other processes that are not related to the task will reduce the points for this task (down to zero).

2. After another cyber attack on the operating system, some negative consequences remained, which are as follows:

- a) the task manager is blocked from time to time;
- b) MS Word program is blocked;
- c) the desktop is locked;
- d) inscriptions appeared instead of time and date on the taskbar;
- e) local disks are hidden.

Task: correct the indicated negative consequences (for each 1 point).

Note: if you delete registry keys and parameters of other services not related to this task, the points for this task will be reduced (down to zero).

3. Given a multi-level folder “TEST” containing directories and subdirectories.

- a) It contains various files with the same hash amount, but located in different directories;
- b) it turned out that 5 files with a similar hash amount are virus downloaders;
- c) These files are protected from normal deletion.

Task: These files should be identified and deleted (1 point for each file).

Note: Deleting other files not related to an assignment will reduce the score for that assignment (down to zero).

4. Given a multi-level folder “TEST” containing directories and subdirectories.

- a) It contains 5 hidden programs;
The hidden program is a PE (Portable Executable) executable file with a changed resolution.
- b) All these files are protected from normal deletion.

Task: You should identify and remove these hidden programs (1 point for each file).

Note: Deleting other files not related to an assignment will reduce the score for that assignment (down to zero).

5. Given a multi-level folder “TEST” containing directories and subdirectories.

a) It contains 5 virus bodies;

The body of the virus is a non-executable file, but it has similarities and extensions with a PE file.

b) All these files are protected from normal deletion.

Task: These virus bodies must be identified and removed (1 point for each file).

Note: Deleting other files not related to an assignment will reduce the score for that assignment (down to zero).

REQUIREMENTS for the program being developed

1. The program developed to solve tasks at this stage must be implemented in a programming language specified in the list of programming languages that can be used at the Olympiad.
2. The developed application must run in the Windows operating system environment.
3. To complete these tasks, a unified program must be developed. The program must be executed as executable machine code (*.exe).
4. The program must be developed as an application with a simple interface that is understandable to the average user and, after submission for verification, does not require compilation in a programming language editor. All 5 tasks must be completed by executing one command or button.
5. The program must have access to the TEST folder located next to it, either through the program dialog, or through the input line, and either by default in the code and not touch any other folders. If the program begins to analyze the entire system or folders not related to the specified folder, the participant will receive 0 points for this stage of the Olympiad.
6. The program execution time should not exceed 1 minute.
7. After completing the tasks, the participant must create a folder, place the source program code (source) and the machine code of the program (executable file) in it, give it a name in the form of his participant code (issued upon registration before the start of the competition and consists of 1 capital letter and two digits). This folder must then be transferred to the jury member via a network or storage medium.

PROCEDURE for conducting and summing up the competition

1. Each participant must be placed at a separate personal computer and registered by issuing a code consisting of one capital letter and two numbers (for example, P34).
2. Before the start of the competition, each participant will receive technical specifications in electronic form (via the network from an accessible folder) or in another way, or in printed form.

3. The competition will be held on two floors of the university library and in 13 computer classrooms of the Faculty of Digital Technologies and Cyber Security. Each computer lab will have a video surveillance system installed and a jury member will be present.
4. During the first 30 minutes, an Olympiad participant can contact the team leader or representatives of the organizing committee and jury about a problem that he does not understand.
5. During the Olympiad, the participant is allowed to bring a pen, pencil and blank paper. With the consent and under the control of the jury members, it is allowed to use reference and information literature in electronic (downloaded to computers only in the presence of jury members) and in paper form. During the Olympiad, it is not allowed to use the Internet, use a telephone, personal laptop or other mobile devices, or consult with other participants.
6. In case of failures in the operating system or in the editor of the programming language used to complete the task on the assigned personal computer, you should not act independently, but contact a representative of the Organizing Committee or members of the jury.
7. If personal needs arise (toilet, water, food, etc.) during the Olympiad, the participant can contact a representative of the organizing committee.
8. A student who violates these requirements will be excluded from the list of participants in this stage of the Olympiad and will be assigned 0 points for this stage.
9. 180 minutes are given to complete the tasks. Participants can complete and submit their assignments in advance. The time spent on completing their tasks is recorded by the jury members in minutes. This time will be added to the time spent in other stages and will be taken into account for equality of points.
10. Programs submitted by participants for evaluation will be transmitted in folders with the name in the form of a participant code via a network or electronic media to jury members or assistants working on several computers. Participants' programs will be launched on problem computers, and then the work of the programs will be assessed by monitoring software, and the test results will be saved in a *.log file with a name that matches the participant's code.
11. *.log files of all participants will be collected from several computers, read by the main judging program and placed in a database, and a preliminary report will be created. This report will be provided to all jury members electronically.